无线物联网中局部有向无环图区块链研究 *

杨昌霖 [1, 2†]，王继光 [1]，汪 清 [3]

(1. 中原工学院 计算机学院，郑州 451191; 2. 中山大学 软件工程学院，广东 珠海 519082; 3. 天津大学 电气自动化与信息工程学院，天津 300072)

摘 要：为了减少无线物联网中数据的存储需求和传输消耗，提出一种基于有向无环图(directed acyclic graph,DAG)的局部有向无环图区块链方案(local DAG blockchain, LDB)。该方案通过使无线物联网节点只需存储本身的数据区块以及邻居节点的区块哈希值，解决了节点的存储限制与传输消耗问题，并在保证数据安全的前提下减少数据验证的过程，提升了网络的整体使用率。同时，提出一种恶意节点检测机制，有效的检测网络中的恶意节点。仿真实验中，通过与 IOTA 在不同网络模型中对比，比较了 LDB 和 IOTA 的存储需求、传输消耗和链路负载。实验结果表明，在网络规模为 500 个节点时，LDB 相比 IOTA 在节点存储空间上减少 99.8%，平均传输消耗降低 66.2%，最大负载减少约 28 倍。

关键词：局部有向无环图区块链；无线物联网；数据完整性

中图分类号：TP311.1 doi: 10.19734/j.issn.1001-3695.2022.02.0063

Local directed acyclic graph blockchain in wireless Internet of Things

Yang Changlin[1, 2†], Wang Jiguang[1], Wang Qing[3]

(1. *School of Computer Science*, *Zhongyuan University of Technology*, *Zhengzhou* 451191, *China*; 2. *School of Software Engineering*, *Sun Yat-Sen University*, *Zhuhai Guangdong* 519082, *China*; 3. *School of Electrical & Information Engineering*, *Tianjin University*, *Tianjin* 300072, *China*)

Abstract: This paper proposed a Local Directed acyclic graph Blockchain (LDB) to reduce the storage and communication requirements of blockchain, which can be applied in Wireless Internet of Things (WIoT) . In the proposed LDB, a WIoT node only needs to store its own generated data and hash values that derived from the data of its neighbor nodes. This enables storage and transmission resources restricted WIoT nodes to operate blockchain. The proposed LDB includes a simple data verification procedure to guarantee data integrity. In particular, this paper proposed a malicious nodes detection mechanism to effectively discover data manipulation. The simulation results show that when there are 500 nodes, LDB reduces the average storage cost by 99.8%, the average transmission cost by 66.2%, and the maximum link capacity by 28 times compared with state-of-art DAG blockchains.

Key words: local directed acyclic graph blockchain; wireless Internet of Things; data integrity

0 引言

物联网是一个涵盖所有与互联网相连事务的总称[1]，随着物联网设备的不断升级与无线通信技术的不断发展，无线物联网在医疗保健、能源、汽车、环保和交通等领域得到广泛应用[2]，根据 Juniper Research 的数据显示，全球连接的无线物联网设备将由 2020 年的 385 亿台增长到 2023 年的 500 亿台[3]，无线物联网设备的不断增加给人们生活带来极大便利的同时，也带来了各种安全问题。无线物联网设备能够生成、处理和交换大量数据和隐私敏感信息[4]，这些数据信息与人们的生活关系密切，此外，无线物联网设备节点之间通过无线连接，安全性较低，并且节点的功率、存储和计算能力有限，导致无线物联网设备的数据容易被攻击者窃取、盗用或伪造虚假身份窜改设备，对人们的生活带来极大的威胁。

区块链作为可融合多种技术的分布式计算和存储系统，以其去中心化、不可窜改、可溯源等特性被广泛应用于无线物联网安全中[5]。此外，区块链使用加密哈希算法对系统中存储的交易实现良好的隐私保护。然而，区块链的安全性依赖其区块链高度冗余的特性，即每个节点需存储完整的交易历史以确保数据的安全[6]。同时，无线物联网设备通常设计简单、内存较小，难以存储区块链的全部数据，以比特币区块链[7]为例，2022 年初，单个节点的存储需求已经接近 380G[8]，这对无线物联网节点的存储空间是一个巨大挑战。

为了降低区块链节点的存储需求问题，目前应用较为广泛的方案有轻节点、压缩区块链、分片区块链和编码区块链[9]。其中，轻节点[7]不存储区块数据，当其验证某一个具体交易时，需依赖普通节点存储的数据，这导致区块链系统分布性降低，造成安全隐患[10]。压缩区块链通过删除部分区块链信息来降低存储需求，节点仅存储验证新区块所需要的交易信息[7]、用户余额[11]或区块摘要[12]，这导致一些区块数据永久丢失，破坏区块链数据完整性。分片区块链[13]将区块链划分为多个子链，其存储需求根据分片数量增加等比例降低。但跨链交易和子链合并等操作对节点功能复杂度要求较高。同时，子链网络节点数量较少会降低子链的安全性[14]。编码区块链[15]利用纠错码技术将区块链数据编码，分布式地存储在节点中。然而，编码区块链需要节点具备强大的编解码计算能力，增加区块链运行成本。

与传统区块链相比，有向无环图(directed acyclic

收稿日期：2022-02-14；修回日期：2022-04-06 基金项目：国家自然科学基金资助项目(61802454)

作者简介：杨昌霖(1990-)，男(通信作者)，河南平顶山人，讲师，硕导，博士，主要研究方向为物联网和区块链(changlin1@outlook.com)；王继光(1995-)，男，河南濮阳人，硕士研究生，主要研究方向为区块链；汪清(1982-)，女，浙江常山人，副教授，博导，博士，主要研究方向为通信雷达一体化、智能信息处理等.

graph,DAG)区块链的高并发性被认为是解决区块链可扩展性问题最具前景的研究方向，并得到学术界和产业界越来越多的关注与重视[16]。同时，也为无线物联网的存储问题带来新的解决思路，例如 IOTA(Internet of Things Application cryptocurrency)[17]、Byteball[18]和 Hashgraph[19]。其中，文献[6]针对资源受限的车载社交网络提出一种基于轻量级的有向无环图区块链，每个节点只将感兴趣的数据存储在感兴趣的主题组中，同时，为了避免具有大量数据的大规模组内带来巨大存储成本，进一步提出了组内的历史数据剪枝方法，减少每个节点中存储的重复数量来满足存储需求。文献[20]提出一种基于有向无环图区块链的 IIoT 结构,并结合微分隐私技术进一步确保数据的隐私和完整性，同时还提出了一种负载平衡算法,有效地平衡节点能耗和网络寿命之间的关系。文献[21]提出一种轻量级、可扩展的无线物联网分布式账本(LSDI)，将大型 P2P 网络划分为较小的 P2P 网络来减少无线物联网的计算开销，并且通过删除足够旧的事务来减少无线物联网中的存储开销，实验表明，LSDI 系统在有效管理无线物联网的存储和计算开销的同时，实现了高事务吞吐量和可扩展性。

文献[22]对基于有向无环图技术的区块链进行分析与比较，得出 IOTA 最适合无线物联网系统，因为它实现了零交易费用，确保数据完整性，同时避免传统区块链易受到的双重支出等攻击。然而，IOTA 是面向交易的区块链，需要对交易进行验证，且区块产生时需复杂的计算权重过程，另一方面，IOTA 具有极快的存储扩张速度，并且在产生新区块时和传统区块链一样需要全网广播，由于无线物联网设备资源的限制，IOTA 无法直接运行在无线物联网节点上。

目前无线物联网应用中，节点并不需要对其他节点采集到的数据进行验证和判断[23]，例如温度、湿度等。这些数据发送到用户时，由用户根据这些数据作出最终决定，例如发起火灾警报[24]、进行人工降雨[25]等。因此，将无线物联网与区块链结合，需要保证数据不被窜改的同时，网络管理员不会因为攻击者修改的数据进行错误的判断。

为了减少无线物联网中数据的存储需求和传输消耗，在确保数据安全的情况下，本文提出一种局部有向无环图区块链方案(local DAG blockchain,LDB)，为资源受限的无线物联网提供安全的数据存储解决方案并具有较低的存储和传输需求。简单来说，LDB 将有向无环图区块链作为无线物联网底层的数据结构，以数据为单位，相比面向块的传统区块链具有更高效和可扩展的特性。与 IOTA 相比，LDB 中节点仅需把数据的摘要发送给物理空间较近的邻居节点，不进行全网广播，降低传输消耗，同时，节点存储自身产生的数据区块以及少量邻居数据区块的摘要，大幅降低网络的存储需求。

1　系统模型

本文提出的 LDB 从区块结构、工作模式、复杂度以及安全性进行优化整合，在确保数据安全的情况下，满足无线物联网节点低能耗低存储的需求，使得该系统具有安全、低资源需求等特点。

传统区块链中，节点需要独立存储所有区块，建立从创始区块到最新区块之间的单向链接，对于无线物联网来说，节点资源有限，难以将所有区块保存在节点中，针对这一问题，将 LDB 划分为物理层面和逻辑层面，即无线物联网和有向无环图区块链两大部分。在物理层面，无线物联网由传感器节点和用户组成，传感器节点仅存储本地产生数据区块和少量邻居摘要信息，减少节点存储需求。在逻辑层面，有向无环图区块链负责将传感器节点收集的数据链接起来，达到不可窜改的目的。本文使用的符号如表 1 所示。

表 1　系统符号

Tab. 1　System symbol

参数	含义
P	数据信息或交易信息
$h(\ )$	计算数据的摘要及区块哈希
f	父区块哈希字节长度
t_{i,Z_i}	传感器节点 i 产生区块 Z 的时间戳
Ad_x	区块 x 的地址
M_x	区块 x 的签名
R	传感器节点的传输半径
$d(i,j)$	传感器节点 i ， j 之间的欧几里德距离
$F(\ )$	区块大小以及字段长度
$\mathcal{N}(\ )$	传感器节点的邻居集合
Z_i	传感器节点 i 产生的区块数量
θ	网络的平均传输消耗
S_i	区块占无线物联网节点 i 的存储空间
$\eta_{i,j}$	传感器节点 i 的邻居 j 的状态区块哈希值

物理层面上，将无线物联网表示为 $G(\mathcal{V},\mathcal{E})$，其中，$\mathcal{V}$ 表示传感器节点的集合，$\mathcal{E}$ 表示传感器节点间的链路集，假设每个节点 $i\in\mathcal{V}$ 都有相同的传输范围 R，如果网络中两个节点 i,j 的欧几里德距离小于他们传输半径之间的最小值，则这两个节点互为邻居，由 $\mathcal{N}(i)$ 表示，其定义为

$$\mathcal{N}(i)=\{j\,|\,d(i,j)<R,\forall j\in\mathcal{V}\} \tag{1}$$

节点集 $\mathcal{V}$ 通过链路集 $\mathcal{E}$ 构成无线物联网。

逻辑层面上，用 $D(\mathcal{B},\mathcal{L})$ 表示基于数据的 DAG 分布式账本结构，其中 $\mathcal{B}=\{b_1,b_2,\cdots,b_n\}$ 表示 D 中数据区块的集合，$\mathcal{B}$ 中的每一个元素 $b_\alpha(\alpha=1,2,\cdots,n)$ 为有向无环图区块链中的数据区块，$\mathcal{L}=\{l_1,l_2,\cdots,l_m\}$ 表示 $\mathcal{B}$ 中数据区块之间的链路集，$\mathcal{L}$ 中的每一个元素 l_k（即 $\mathcal{B}$ 中某两个元素 b_α,b_β 的有序对）记为 $l_k=(b_\alpha,b_\beta)(k=1,2,\cdots,m)$，表示数据区块之间的链路。对于任意一个节点 $b_\alpha\in\mathcal{B}$，都不存在一条路径 $(l_1,l_2,\cdots,l_m),l_k\in\mathcal{L}$ 使得从 $\mathcal{B}$ 出发到 $\mathcal{B}$ 终止，即数据区块之间建立一个有向无环图。

用 $b<i,t_{i,Z}>$ 表示传感器节点 i 在时间 t_{i,Z_i} 产生的区块，其中 Z_i 是该节点产生的最新区块序号，设置 $b<i,t_{i,Z_i-1}>$ 为该传感器节点 i 的当前状态区块，$h(b<i,t_{i,Z_i-1}>)$ 为该区块哈希值。每个节点 i 的第 1 组区块 $b<i,t_{i,1}>$ 为初始区块，使用 $\eta_{i,j}$ 表示为传感器节点 i 邻居节点 j 的当前状态区块的哈希值，所以，$\eta_{i,j}=h(b<i,t_{i,Z_i-1}>)$，假设节点 i 数据生成的速率为 r_i，当其产生 P 字的数据时即打包为一个区块，区块数据部分大小为 $F(P)$，其中，时间戳 t_{i,Z_i} 由下式计算

$$t_{i,Z_i}=\frac{Z_i\times F(P)}{r_i} \tag{2}$$

LDB 区块链示例如图 1 所示。图 1 上半部分是由三个节点 1,2,3 各产生 3 个区块共 9 个区块的有向无环图区块链，可以转换为传统的有向无环图区块链，例如文献[17]中 IOTA 的共识机制 Tangle，如下半部分所示，即 $b_1=b<1,1>$，$b_2=b<2,1>$ … $b_9=b<3,3>$。

2　局部有向无环图区块链(LDB)

在本节中，首先分析 IOTA 的区块结构，然后讨论基于 IOTA 的无线物联网系统的存储空间与传输消耗，接着提出 LDB 的区块结构，并提出 LDB 的工作模式以及传感器节点的存储空间与传输消耗，最后分析 LDB 的安全性。

2.1　IOTA 区块结构

IOTA 中，交易是基本数据单元，每个区块包含有一个交易，全部区块的组合包含交易的所有相关信息，以 IOTA 为例的有向无环图区块链区块结构如图 2 所示，IOTA 区块主要由区块地址、Tag、两个父区块哈希值、时间戳、nonce、

Bundle、签名和信息列表组成，根据使用场景的不同，信息列表不同，在加密货币中为交易的信息，在无线物联网设备中则为需要存储的数据。与单链区块链不同的是，IOTA 的每个区块中包含两个父区块哈希值。

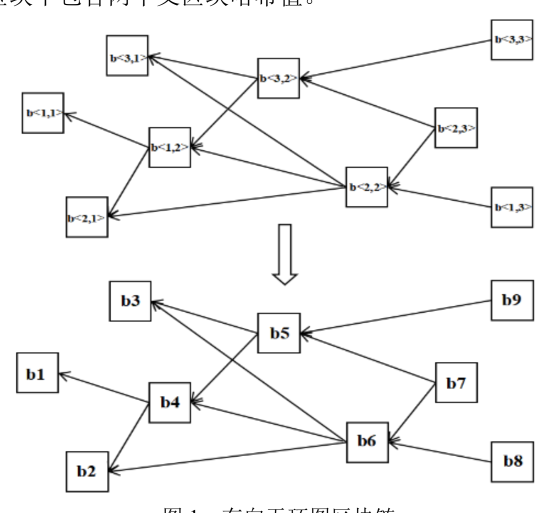


图 1　有向无环图区块链

Fig. 1　DAG blockchain



图 2　IOTA 区块结构　　　图 3　LDB 区块结构

Fig. 2　IOTA block structure　　　Fig. 3　LDB block structure

当传感器节点采集到的一组新的数据时，就有了生成区块的需求。其中，区块地址用来唯一表示该区块，Tag 为交易标签，Bundle 为交易的单位，父区块哈希值用来将该区块与其他区块相链接，时间戳不能更改，用来记录当前时间区块发生的事情，同时增加窜改区块的难度；签名方法使用 Winternitz one-time signature (W-OTS)签名算法，这是一种后量子签名算法，可以抵御量子攻击；工作量证明是传感器节点产生数据区块时查找 nonce，以避免恶意节点的泛洪攻击，且该工作量证明只是一个定量，不会像区块链的工作量证明一样产生很多额外的交易费用[16]；数据信息部分就是用来存储传感器节点采集到的数据内容。

IOTA 中一个区块 b_i 的大小为

$$F_{IOTA}=F(Ad_{b_i})+F(Tag)+F(t_{i,Z_i})+F(Bundle)+2F(f)+F(nonce)+F(M_{b_i})+F(P) \tag{3}$$

在基于 IOTA 的传感网节点中，区块占传感网节点的存储空间计算公式为

$$S_1=S_2=\cdots=S_i=\sum_{i\in\mathcal{V}}\sum_{Z=1}^{Z_i}F\left(b<i,t_{i,Z_i}>\right) \tag{4}$$

每个传感器节点在产生一个区块时要将新区块发送到所有节点 $\mathcal{V}$，所以 IOTA 的平均传输消耗为

$$\theta=\frac{\sum_{i\in\mathcal{V}}\sum_{Z=1}^{Z_i}|\mathcal{E}|F\left(b<i,t_{i,Z_i}>\right)}{|\mathcal{E}|} \tag{5}$$

2.2　LDB 区块结构

考虑到在实际的无线物联网应用中，节点并不需要验证网络中其他节点的历史数据[23]，为了使 LDB 更适用于无线物联网，本节重新定义了 LDB 区块的结构。与 IOTA 不同，LDB 存储和传输的是数据信息，所以 LDB 区块结构删除了 IOTA 中与交易相关的 Tag 和 Bundle 两部分，并将交易信息改为数据信息，然而，由于节点需要存储来自邻居节点的摘要信息，所以将原本 IOTA 中区块的两个父区块哈希值扩展为 $|\mathcal{N}(i)|$ 个父区块哈希值，同时保留了区块的一些基本结构。因此，LDB 区块的结构包括区块地址、$|\mathcal{N}(i)|$ 个父区块哈希值、时间戳、nonce、签名和数据信息，如图 3 所示。

LDB 中一个区块 b_i 大小为

$$F_{LDB}=F(Ad_{b_i})+F(t_{i,Z_i})+|\mathcal{N}(i)|F(f)+F(nonce)+F(M_{b_i})+F(P) \tag{6}$$

与 IOTA 类似，LDB 区块结构同样需要父区块哈希值，不同之处在于 LDB 区块包含 $|\mathcal{N}(i)|$ 个父区块哈希值，$|\mathcal{N}(i)|$ 的值取决于区块所属传感器节点 i 的邻居传感器节点数量。因此 LDB 区块也可以保证数据的安全，抵御女巫攻击、重放攻击和 DDoS 攻击。

2.3　LDB 工作模式

在 LDB 中，当传感器节点收集到一定的数据时，只需要对其邻居传感器节点进行广播，不需要对全网广播，而且每个传感器节点不需要存储网络中所有的数据信息，只需要存储自己的区块和邻居节点广播给自己的区块哈希值。下面是 LDB 的工作模式。

1)传感器节点 i 在一定时间内采集到数据 P；

2)根据数据地址的私钥获取区块签名；

3)传感器节点 i 将其存储的邻居节点最新状态区块哈希 $\eta_{i,j}; j\in\mathcal{N}(i)$ 作为父哈希值 f，然后做一定量的工作量证明查找合适的 nonce 值；

4)传感器节点 i 将 P、区块地址、$|\mathcal{N}(i)|$ 个父节点哈希值 f、nonce、签名、时间戳 t_{i,Z_i} 组成新的区块 $b<i,t_{i,Z_i}>$，接着在对新区块进行哈希计算，得到 $h(b<i,t_{i,Z_i}>)$，将 $h(b<i,t_{i,Z_i}>)$ 广播给传感器节点 i 的邻居节点 $j\in\mathcal{N}(i)$，同时传感器节点 i 将 $b<i,t_{i,Z_i}>$ 以及传感器节点 i 与邻居节点 $j\in\mathcal{N}(i)$ 的链接信息存储在本地；

5)邻居节点 $j\in\mathcal{N}(i)$ 将接收到的 $h(b<i,t_{i,Z_i}>)$ 保存在本地存储单元并更新邻居状态区块，$\eta_{i,j}=h(b<i,t_{i,Z_i}>)\leftarrow h(b<i,t_{i,Z_i-1}>)$; $j\in\mathcal{N}(i)$。

图 4 为 LDB 工作流程的示例图，为了简化符号，把区块表示为 b_i，同时，$\mathcal{N}(A)=\{B,C\}$，$\mathcal{N}(E)=\{D\}$。当传感器节点 E 采集一组 P 后，根据数据地址的私钥对区块签名，然后将传感器节点 D 当前状态区块 b_5 的哈希值并进行一定量的工作量证明查找到 nonce，将 $h(b_5)$、P、$Ad_{b_{12}}$、$M_{b_{12}}$、nonce 和 t_{E,Z_E} 打包成区块 b_{12}，然后计算 $h(b_{12})$，并将 $h(b_{12})$ 广播给传感器节点 D，当传感器节点 D 接收到 $h(b_{12})$ 后更新 $\eta_{D,E}=h(b_{12})$。同样，传感器节点 A 采集一组 P 后，根据交易地址的私钥对区块签名，然后将传感器节点 B 和 C 当前状态区块 b_{10} 和 b_{11} 的哈希值并进行一定量的工作量证明查找到 nonce，将 $h(b_{10})$、$h(b_{11})$、P、$Ad_{b_{13}}$、$M_{b_{13}}$、nonce 和 t_{A,Z_A} 打包成区块 b_{13}，然后计算 $h(b_{13})$，并将 $h(b_{13})$ 转发给传感器节点 B 和传感器节点 C，当传感器节点 B 和传感器节点 C 接收到 $h(b_{13})$ 后更新 $\eta_{A,B}=h(b_{13})$，$\eta_{A,C}=h(b_{13})$。每个传感器节点只需向其邻居节点发送区块，不需要进行全网广播，邻居节点之间形成一个局部的区块链系统，但是所有节点的区块数据组成一个完整的有向无环图区块链，保证了数据的安全。

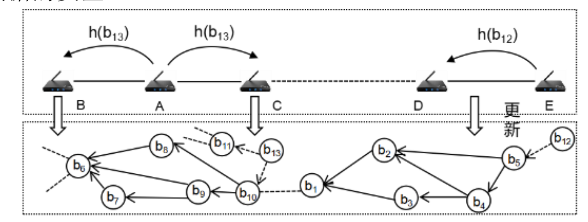


图 4　LDB 工作模式图

Fig. 4　LDB working mode diagram

网络中的所有数据会通过邻居节点之间哈希摘要相互链接形成一个有向无环图区块链，在此基础上，提出一种恶意节点检测机制，当用户在收集传感器节点 i 中数据时，用户会验证邻居节点 $j\in\mathcal{N}(i)$ 发送的 $h(b<j,t_{j,Z_j}>)$ 与传感器节点 i 接收的 $h(b<j,t_{j,Z_j}>)$ ，当 $j.h(b<j,t_{j,Z_j}>)\neq i.h(b<j,t_{j,Z_j}>)$ 时，则说明传感器节点 i 可能会被恶意攻击，这种机制使基于 LDB 的无线物联网系统数据与传统的有向无环图区块链具有同样的安全性。

在采用 LDB 的传感网节点中，区块占传感网节点的存储空间计算公式为

$$S_i^{'}=\sum_{Z=1}^{Z_i}F\left(b<i,t_{i,Z_i}>\right)+\sum_{Z=1}^{Z_j}F\left(h\left(b<j,t_{j,Z_j}>\right)\right);i\in\mathcal{V},j\in\mathcal{N}(i) \tag{7}$$

在 LDB 中，每个新区块仅发送其哈希到邻居节点，因此，平均传输消耗的公式为

$$\theta^{'}=\frac{\sum_{i\in\mathcal{V}}\sum_{Z=1}^{Z_i}F\left(h\left(b<i,t_{i,Z_i}>\right)\right)\times|\mathcal{N}(i)|}{|\mathcal{E}|} \tag{8}$$

2.4　存储与传输复杂度分析

为了评估 LDB 的性能，本文对两种方法在存储和传输消耗上的对比进行研究。

已知网络中传感器节点数量为 $|\mathcal{V}|$，每个区块由区块头和区块体组成，例如在比特币中，区块头包含的为创建区块的元数据与前一个区块的链接，区块体为所有交易信息。由于区块体远大于区块头[17]，假设存储和传输区块体的复杂度为 $\mathcal{O}(1)$ ，假设存储和传输区块头的复杂度为 $\mathcal{O}(\alpha)$，$1\gg\alpha\to 0$ 。IOTA 的存储和传输复杂度是 $\mathcal{O}(|\mathcal{V}|(1+\alpha))$ ，在 LDB 中，每个节点存储所有区块头以及自己产生的数据，即极小一部分区块体。同时，LDB 中节点也只需向邻居节点发送区块头和区块体，不需进行全网广播。因此，LDB 的存储复杂度是 $\mathcal{O}(1+\alpha)$ ，传输复杂度是 $\mathcal{O}(|\mathcal{N}(i)|(1+\alpha))$ 。在最恶劣条件下，网络中全部节点互为邻居，即 $|\mathcal{V}|=|\mathcal{N}(i)|$，此时，LDB 的存储复杂度远小于 IOTA，传输复杂度相同。然而，在实际无线物联网网络中，全部节点互为邻居节点的概率很低，$|\mathcal{N}(i)|$ 远小于 $|\mathcal{V}|$，因此 LDB 的实际传输复杂度小于 IOTA(见实验 3.5 和 3.6)。

2.5　安全性分析

本章节分析 LDB 在无线物联网中的安全性，并讨论了三种攻击模式，具体内容如下。

1)抵抗女巫攻击

在 P2P 网络中如果存在一个恶意节点，那么该恶意节点可以具有多重身份，并且利用多重身份伪装成大量节点，在这种情况下，它们可以拒绝接收或传输区块，从而有效阻止其他用户进入网络，当攻击者已控制系统中 51%的节点，在这种情况下，它们可以轻易更改交易的顺序，并防止交易被确认。在 LDB 系统中，当网络存在至少一个诚实节点时，哈希摘要在诚实节点逻辑有向无环图中的链接存在断路，从而发现攻击。假设无线物联网中传感器节点 i 被攻击，导致网络中存在大量的恶意节点，攻击者向网络中发送虚假数据哈希摘要，将 $h(b<i,t_{i,Z_i}>)$ 改为 $h^{'}(b<i,t_{i,Z_i}>)$ ，若其邻居传感器节点 j 为诚实节点，则 j 中存在区块 $b<j,t_{j,Z_j}>$ 且 $t_{j,Z_j}>t_{i,Z_i}$ ，其中父区块哈希 $h(b<i,t_{i,Z_i}>)\neq h^{'}(b<i,t_{i,Z_i}>)$ 。因此，网络管理员获取节点 j 的数据后能够发现逻辑有向无环图链接错误。此外，LDB 在节点形成区块时也会进行一个定量的工作量证明来确保区块的有效性，所以 LDB 可以抵抗女巫攻击。

2)抵抗重放攻击

重放攻击指攻击者发送一个目的节点已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。重放攻击可以由发起者，也可以由拦截并重发该数据的敌方进行。攻击者利用网络监听或者其他方式盗取认证凭据，之后再把它重新发给认证服务器。LDB 中传感器节点 i 每产生一个区块 $b<i,t_{i,Z_i}>$，都会带有一个时间戳 t_{i,Z_i}，并且只需将 $h(b<i,t_{i,Z_i}>)$ 广播给 $\mathcal{N}(i)$ ，使得数据传输时延小，容易做到精准的时间同步，即使是大型网络也不会受影响，例如在图 4 中，传感器节点 A 被攻击者攻击，将之前发送给传感器节点 B 和 C 的区块哈希 $h(b_{13})$ 重新发送，第一次发送 $h(b_{13})$ 时时间戳为 t_{A,Z_A} ，再次发送时时间戳为 $t^{'}_{A,Z_A}$ ，由于 $h(b_{13})$ 相同，$t_{A,Z_A}\neq t^{'}_{A,Z_A}$ ，所以传感器节点 B 和 C 可以拒接接收重复发送的 $h(b_{13})$ ，从而有效抵抗重放攻击。

3)抵抗 DDoS 攻击

DDoS 攻击指处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。在 LDB 中，每个区块都有属于自己的时间戳 t_{i,Z_i}，如果攻击者在一个传感器节点上同时发送大量区块的话，很容易被发现，同时传感器网络大都为廉价设备，如果发现网络中有传感器节点已经被恶意攻击，可以将被攻击节点更换为新的传感器节点。所以 DDoS 攻击对其的影响不大。

3　实验

3.1　实验环境

本文实验在 Pycharm，Python3.7 环境上进行仿真实验的代码编写，所有仿真实验均在 Intel Core i7-7500u CPU，8Gb 内存的 Windows10 系统中运行。为了确保实验的准确性，每个实验数据均取自于 100 个独立仿真实验的均值。

3.2　主要参数设置

为了充分探讨 LDB 在无线物联网中的性能，本文在仿真实验中，以有向无环图区块链为基础，实现所提出的 LDB 方案，并通过与 IOTA 对比，验证 LDB 的可行性。为了使实验结果更具代表性，网络模型采取随机组合方式，然后分别给定网络中传感器节点的传输范围 $R=20$ m，在半径为 50m 的圆形范围内随机放置传感器节点，传感器节点采集数据的平均速率为 $r_i^{'}=50$ bit/s，由于 IOTA 的尺寸较小[27]，实验中设置一组固定大小的区块 $F(b<i,t_{i,Z_i}>)=1024$ bit，区块的哈希长度为 $f=h(F(h(b<i,t_{i,Z_i}>)))=256$ bit，区块的数据部分为 $F(P)=500$ bit，所以平均生成一个区块的时间为 $t_{i,Z_i}\div Z_i=10$ s。在 IOTA 中，传感器节点广播区块采用的是 gossip 算法，节点将更新的账本状态发送给邻居节点，每个节点将请求与其当前已知的分类帐版本进行比较，并再次检查是否存在冲突。如果没有发现冲突，节点更新它的账本状态并再次将更新后的状态发送给他的邻居。在基于 LDB 的无线物联网系统中，节点只需将区块发送给其邻居节点，简化了广播的过程。

首先，由于 LDB 相对比 IOTA 区块头多存储 $|\mathcal{N}(i)|-2$ 个哈希值，因此实验 3.3 展示区块头相比数据部分对节点存储空间有很小的影响。实验 3.4 中对比 LDB 和 IOTA 中区块头对节点存储的影响，并显示了两种方法下节点存储量的比值。接下来的实验 3.5 在随机的无线物联网中评估了 LDB 与 IOTA 存储量和传输消耗上的差异，其中存储的对比可以明显看出 LDB 的存储量远小于 IOTA。最后，实验 3.6 对两种方法下网络的链路负载情况进行分析与比较。

3.3　区块头对存储空间的影响

首先，在数据的分布情况中，为了使实验更具真实性，数据产生速率为泊松分布，实验假设网络最初有 $\mathcal{V}=500$ 个节点，网络中一共生成 $Z=1000$ 个区块，在图 5 中展示了传感器节点数据分布情况。由于 LDB 区块中父哈希值的数量要大于 IOTA 中区块头的 2 个父哈希值，所以进一步分析区块头对节点存储空间的影响，根据式(5)(8)，记录了使用 LDB 与 IOTA 的传感器节点的比值，并在图 6 中显示不同比值出现的频率，实验结果表明，在网络节点 $\mathcal{V}=500$ 时，区块头比值相比较没有区块头也只增加 0.1%，并会随着网络规模的变大

比值缩小，所以区块头对节点整体存储量的影响不大。

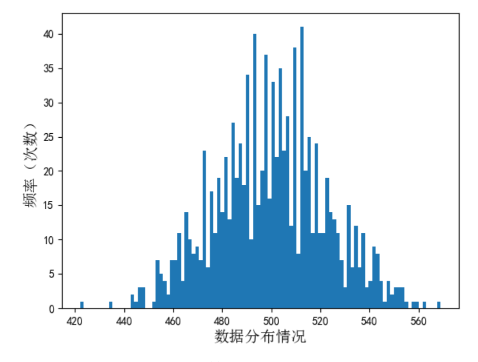


图 5　数据泊松分布

Fig. 5　Poisson distribution of data

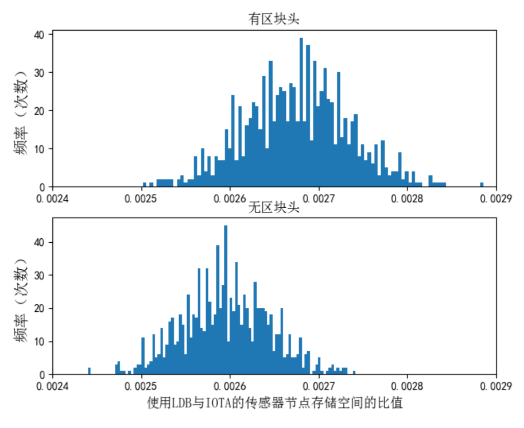


图 6　区块头对节点存储空间的影响

Fig. 6　The impact of block headers on node storage space

3.4　节点存储量比较与分析

图 7 描述了在无线物联网中 LDB 和 IOTA 的节点存储量的总体趋势对比。实验假设网络中有 $\mathcal{V}=500$ 个传感器节点，每个传感器节点产生 $Z=40$ 个区块。根据式(4)(7)结合图 7 可以看出节点存储量随着传感器节点不断的采集数据区块和接收到其他节点发送过来的区块不断增加，两种方法的总体趋势都是逐渐增加，当时间戳 $t_{i,z_i}=50$ h 时，采用 LDB 的无线物联网的节点存储量约为 $S_i'=3.9\times10^4$ bit，采用 IOTA 的无线物联网的节点存储量约为 S_i=2.0×10^7 bit，采用 IOTA 的无线物联网的节点存储量约为 LDB 的节点存储量的 500 倍，随着节点个数的增加，采用 LDB 的无线物联网的节点存储量相对比 IOTA 呈网络节点规模数减少。这是由于 IOTA 在节点广播区块时，网络中的每个节点都需要进行本地存储，即网络中的每一个节点都需要存储所有的区块，而采用 LDB 的无线物联网中的每个节点只需存储来自于其邻居节点的哈希值即可。实验结果表明，相对比 IOTA，LDB 可以减少无线物联网中节点存储空间的 99.8%，且当无线物联网中节点个数越多，减少比例越大。

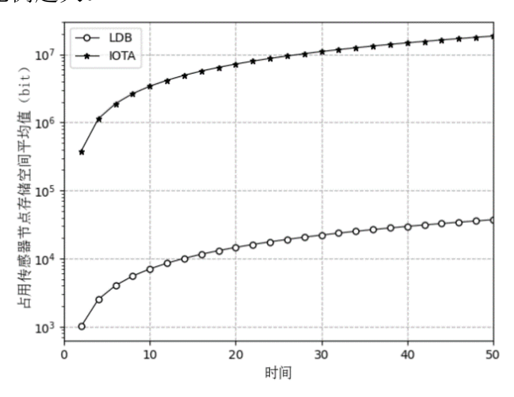


图 7　两种方法下存储空间的比较

Fig. 7　Comparison of storage space under the two methods

3.5　传输消耗比较与分析

图 8 显示了无线物联网中 LDB 和 IOTA 平均传输消耗的整体趋势对比，主要分析区块的大小对传输消耗上的影响，在式(5)(8)中，采用 LDB 的无线物联网中链路是指邻居节点之间的链路，而采用 IOTA 的无线物联网中链路指全网链路。整体趋势表明，随着时间的不断增多，两种方法的传输消耗都在不断增加，但是 LDB 的传输消耗要远小于 IOTA，当时间戳 $t_{i,z_i}=50$ h 时，采用 LDB 的无线物联网的平均传输消耗约为 $\theta'=1.96\times10^6$ bit，采用 IOTA 的无线物联网的平均传输消耗约为 $\theta=5.81\times10^6$ bit，平均传输消耗降低约为 66.2%。原因是 IOTA 在节点在采集到的数据并打包成区块后，会将自己的区块发送给邻居节点，邻居节点在接收到区块后，会再向其邻居节点的邻居节点转发，如此循环下去，直到网络中的所有节点都接收到该节点发送的区块，而 LDB 则只需将区块哈希值发送给邻居节点即可，不用发送到全网的节点。实验结果表明，相对比 IOTA，LDB 可以减少区块在传输中平均传输消耗的 66.2%。

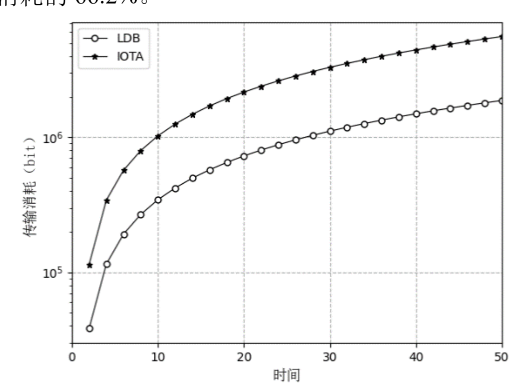


图 8　两种方法下传输消耗的比较

Fig. 8　Comparison of transmission consumption under the two methods

3.6　链路负载比较与分析

在图 9 中，描述了两种方法下链路流量的变化情况，即每条链路上经过的区块数量。实验假设网络规模为 $\mathcal{V}=100$ 个传感器节点，一共产生 $Z=2000$ 个区块和 $\mathcal{E}=1500$ 条链路，然后给每条链路一个编号，由图中可以在采用 IOTA 的无线物联网中看出链路 1 传输的区块数量最多，约为 2000 个，而且链路的分布没有规律且流量很大，在采用 LDB 的无线物联网中，链路流量较为平均，说明 LDB 相对于 IOTA 而言，不会对网络链路造成过高负载。实验结果表明，LDB 相比 IOTA 链路最大负载减少约 28 倍，LDB 可以有效的解决无线物联网中链路拥堵问题，同时减少网络链路的负载。

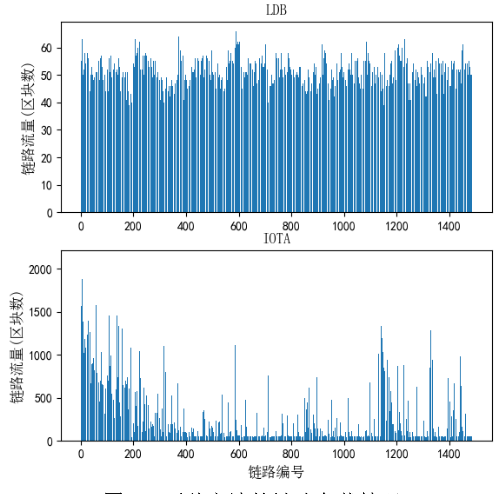


图 9　两种方法的链路负载情况

Fig. 9　The link load of the two methods

4 结束语

本文研究了基于有向无环图区块链的无线物联网数据安全传输方案，一方面，提出一个安全的无线物联网数据传输模型(LDB)，利用区块链技术实现了无线物联网中数据的不可窜改。另一方面，LDB 引入有向无环图区块链技术并将其拆分到局部节点中，取消数据全网验证的过程，不仅减少了无线物联网中节点的存储空间需求，也解决了节点间数据的传输消耗问题。最后，与 IOTA 相比，LDB 有效提高网络整体的吞吐量，在链路流量分布情况中，LDB 明显优于 IOTA。

未来工作将继续研究区块链在物联网领域的数据安全问题，尤其是在无线物联网领域。为了解决有向无环图区块链的存储瓶颈问题，需要针对有向无环图区块链的存储技术进行提升研究，目前，本文给出 IOTA 与 LDB 在安全和性能方面的分析，后面将继续研究 LDB 应用到无线物联网中的具体实现过程。考虑到无线物联网的特点，在下一步的工作中，可以考虑在该模型中给每一个节点设置信用评分机制来检测节点被攻击的可能性。

参考文献：

[1] 史慧洋，刘玲，张玉清. 物链网综述：区块链在物联网中的应用 [J]. 信息安全学报，2019, 4 (5): 76-91. (Shi Huiyang, Liu Ling, Zhang Yuqing. A review of BoT: Blockchain for the Internet of Things [J]. Cyber Security, 2019, 4 (5): 76-91.)

[2] Chen Min, Hao Yixue. Task offloading for mobile edge computing in software defined ultra-dense network [J]. IEEE Journal on Selected Areas in Communications, 2018, 36 (3): 587-597.

[3] Fakhri D, Mutijarsa K. Secure IoT communication using blockchain technology [C]// the International Symposium on Electronics and Smart Devices (ISESD) . Indonesia: Bandung. IEEE, 2018: 1-6.

[4] Qu Chao, Tao Ming, Zhang Jie, *et al.* Blockchain based credibility verification method for IoT entities [J]. Security and Communication Networks, 2018: 1-11.

[5] Restuccia F, Kanhere S D, Melodia T, *et al.* Blockchain for the internet of things: Present and future [J]. arXiv preprint arXiv: 1903. 07448, 2019.

[6] Yang Wenhui, Dai Xiaohai, Xiao Jiang, *et al.* LDV: A lightweight DAG-based blockchain for vehicular social networks [J]. IEEE Transactions on Vehicular Technology, 2020, 69 (6): 5749-5759.

[7] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [DB/OL]. (2008-10-31) [2019-10-02]. http://bitcoin. org, 2008.

[8] Blockchain. BlockchainCharts [EB/OL]. (2022) [2022-04-04]. https://www. blo ckchain. com/charts.

[9] 孙知信，张鑫，相峰，等. 区块链存储可扩展性研究进展 [J]. 软件学报，2021, 32 (1): 20. (Sun Zhixin, Zhang Xin, Xiang Feng, *et al.* Survey of Storage Scalability on Blockchain [J]. Journal of Software, 2021, 32 (1): 1-20)

[10] Karame G O, Androulaki E. Bitcoin and blockchain security [M]. [S. 1.] : Artech House, 2016.

[11] Nadiya U, Mutijarsa K, Rizqi C Y. Block summarization and compression in bitcoin blockchain [C]// the International Symposium on Electronics and Smart Devices (ISESD) . IEEE, 2018: 1-4.

[12] Kim T, Noh J, Cho S. SCC: Storage compression consensus for blockchain in lightweight IoT network [C]// the IEEE International Conference on Consumer Electronics (ICCE) . IEEE, 2019: 1-4.

[13] Zamani M, Movahedi M, Raykova M. Rapidchain: Scaling blockchain via full sharding [C]// Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018: 931-948.

[14] Das S, Kolluri A, Saxena P, *et al.* On the security of blockchain consensus protocols [C]// International Conference on Information Systems Security. Springer, Cham, 2018: 465-480.

[15] Dai Mingjun, Zhang Shengli, Wang Hui, *et al.* A low storage room requirement framework for distributed ledger in blockchain [J]. IEEE Access, 2018, 6: 22970-22975.

[16] 高政风，郑继来，汤舒扬，等. 基于 DAG 的分布式账本共识机制研究 [J]. 软件学报，2020, 31 (4): 1124-1124. (Gao Zhengfeng, Zheng Jilai, Tang Shuyang, *et al.* State-of-the-art survey of consensus mechanisms on dag-based distributed ledger [J]. Ruan Jian Xue Bao/Journal of Software, 2020, 31 (4): 1124-1142.

[17] Popov S. The tangle [J]. White paper, 2018, 1 (3) . https://www. iota. hr/main/media/docs/IOTA_Whitepaper. pdf.

[18] Churyumov A. Byteball: A decentralized system for storage and transfer of value [J]. https://byteball. org/Byteball. pdf, 2016.

[19] Baird L. The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance [J]. Swirlds, Inc. Technical Report SWIRLDS-TR-2016, 1.

[20] Zeng Pengjie, Wang Xiaoliang, Dong Liangzuo, *et al.* A Blockchain Scheme Based on DAG Structure Security Solution for IIoT [C]// the IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) . IEEE, 2021: 935-943.

[21] Cherupally S R, Boga S, Podili P, *et al.* Lightweight and Scalable DAG based distributed ledger for verifying IoT data integrity [C]// the International Conference on Information Networking (ICOIN) . IEEE, 2021: 267-272.

[22] Bhandary M, Parmar M, Ambawade D. A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle [C]// the 5th International Conference on Communication and Electronics Systems (ICCES) . 2020: 1124.

[23] 郭才，李续然，陈炎华等. 区块链技术在物联网中的应用概述 [J]. 物联网学报，2021, 5 (1): 72-89. (Guo Cai, Li Xuran, Chen Yanhua, *et al.* Blockchain technology for Internet of things: an overview [J]. Chinese Journal on Internet of Things, 2021, 5 (1): 72-89.)

[24] Mahgoub A, Tarrad N, Elsherif R, *et al.* IoT-based fire alarm system [C]// the Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4) . IEEE, 2019: 162-166.

[25] Malhotra A, Som S, Khatri S K. IoT based predictive model for cloud seeding [C]// amity international conference on artificial intelligence (AICAI) . IEEE, 2019: 669-773.

[26] Sarfraz U, Alam M, Zeadally S, *et al.* Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions [J]. Computer Networks, 2019, 148: 361-372.